

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230405.1 | 5 апреля 2023 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Cloud Foundry Foundation cflinuxfs3

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	cflinuxfs3: до 0.360.0
Дата выявления	4 апреля 2023 г.
Дата обновления	4 апреля 2023 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-1851 CVE-2022-1927 CVE-2022-2175 CVE-2022-2183 CVE-2022-2126 CVE-2022-2124 CVE-2022-2206 CVE-2022-2581 CVE-2022-2845	<p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H</p> <p>CWE-125: Чтение за пределами буфера</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	7.8

<p>MITRE: CVE-2022-1942 CVE-2022-2125 CVE-2022-2344 CVE-2022-2571 CVE-2022-2849</p>	<p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H</p> <p>CWE-122: Переполнение буфера в динамической памяти</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	<p>7.8</p>
<p>MITRE: CVE-2022-2129</p>	<p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H</p> <p>CWE-787: Запись за границами буфера</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	<p>7.8</p>
<p>MITRE: CVE-2022-1898 CVE-2022-1968 CVE-2022-2345 CVE-2022-2946</p>	<p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой использования после освобождения.</p> <p>CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H</p> <p>CWE-416: Использование после освобождения</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	<p>7.8</p>

<p>MITRE: CVE-2022-0413</p>	<p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного файла. Уязвимость обусловлена ошибкой использования после освобождения.</p> <p>CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-416: Использование после освобождения</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	<p>8.4</p>
<p>MITRE: CVE-2022-2304</p>	<p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H</p> <p>CWE-121: Переполнение буфера в стеке</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	<p>7.8</p>
<p>Ссылки на источники http://github.com/cloudfoundry/cflinuxfs3/releases/tag/0.360.0</p>		